UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,375	08/20/2003	Keith Ballinger	13768.454	7425

47973 7590 07/30/2007

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER
SAN JUAN, MARTINJERIKO P

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/645,375	BALLINGER ET AL.	
	Examiner	Art Unit	
	Martin Jeriko P. San Juan	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-14,17-24,26-29,32 and 33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-14,17-24,26-29,32 and 33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to Applicant's remarks filed on April 9, 2007.

Claims 1-31 were originally pending.

Claims 1-3, 5-8, 10-11, 14-19, 21-22, and 28-31 were rejected; and 4, 9, 12-13, 20, and 23-27 were allowed on the first action filed on January 8, 2007.

Claims 1, 6, 14, 17, 19, 26, and 29 have been amended to incorporate allowable subject matter; claims 4, 15-16, 22, 25, and 30-31 have been cancelled; new claims 32-33 have been added by the Applicant.

Claims 1-3, 5-14, 17-24, 26-29, and 32-33 are now pending in the application.

Amendments to the Specification have been accepted.

Allowable Subject Matter

1. The indicated allowability of claims 4, 9, 12-13, 20, and 23-27 is withdrawn in view of the newly discovered reference(s) to de Jong et al. [US Pub No. 2004/0054628 A1] and further in view of Barrus et al. [US Pub No. 2003/0204721 A1]. Rejections based on the newly cited reference(s) follow. The delay in presenting the newly discovered art is regretted.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

1. Claim 1-3, 5-14, 17-24, 26-29, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Jong et al. [US Pub No. 2004/0054628 A1] and further in view of Barrus et al. [US Pub No. 2003/0204721 A1].

Regarding claim 1, de Jong et al. teaches a computerized network environment including two or more computer systems sending messages [Authenticated Digital Content Request (US Pub No. 2004/0054628 A1, Pg 6, Par 0101)] through a network communication protocol, a method of receiving secure messages [the message comprise the actual request and information generating valid tokens (US Pub No. 2004/0054628 A1, Pg 6, Par 0101)] using custom security tokens [an Authenticated Digital Content Request may comprise a token pool – several customized security tokens organized as chains (US Pub No. 2004/0054628 A1, Pg 6, Par 0101) (US Pub No. 2004/0054628 A1, Pg 7, Par 0112)], the method comprising: an act of identifying one or more security tokens in a received message [Token Chain ID, offset, token type

indicator, (US Pub No. 2004/0054628 A1, Pg 10, Par 0137) – the act of identifying is inherent.], and a value type corresponding with each identified security token [Token Chain ID, offset, token type indicator, (US Pub No. 2004/0054628 A1, Pg 10, Par 0137)] wherein the one or more security tokens are represented in the message by a markup language identifier [The message includes information for use in generating a token pool, as such this includes token type indicators (US Pub No. 2004/0054628 A1, Pg 6, Par 0101)], and wherein the at least one identified security token is identified by the markup language identifier [Token type indicator specifies format of token – (US Pub No. 2004/0054628 A1, Pg 10, Par 0138)]; an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access [Content Repository validates the authenticated digital content request to process the request – the act of matching is inherent in order to access security information, and request parameters and specifications embedded in the tokens (US Pub No. 2004/0054628 A1, Pg 11, Par 0151) (US Pub No. 2004/0054628 A1, Pg 7, Par 0112)]; an act of receiving data from the at least one identified security token into the stored value type that has been matched, wherein the raw data includes one or more of identification information, and a custom property ["custom property" interpreted as "customizable property"] [US Pub No. 2004/0054628 A1, Pg 7, Par 0112]; De Jong et al. does not teach security tokens in a received message that has been encrypted, and an act of decrypting an encrypted portion of the received message based at least in part on the raw data received from the at least one identified security tokens. Barrus et al. teach the use of tokens in encrypted messaging.

Barrus et al. teach security tokens in a received message that has been encrypted [US Pub No. 2003/0204721 A1, Pg 1, Par 0010], and an act of decrypting an encrypted portion of the received message based at least in part on the raw data received from the at least one identified security tokens [US Pub No. 2003/0204721 A1, Pg 3, Par 0027].

It would have been obvious to one of ordinary skill in the art at the time of invention to add another layer of security in the method of sending authenticated digital content request of de Jong et al. by using additional security tokens to encrypt digital content request messages as taught by Barrus et al. because authenticated digital content request has information that include token pool information used for validation [US 2004/0054628 A1, Pg 6, Par 0101] that can be encrypted using additional security tokens to enable a more secure transaction between requesting user media devices and content providers. The suggestion/motivation for combining would have been to prevent an entity other than the intended recipient from accessing the message [US 2003/0204721 A1] thereby protecting the user's interest since an authenticated digital content request has information about the user's token pool. De Jong et al. and Barrus et al. are analogous art because they are both in the same field of endeavor involving messaging using security tokens. Therefore, it would have been obvious to combine the inventions of De Jong et al. and Barrus et al.

Regarding claim 2, the use of digital signatures for authentication is well known in the art of digital security. It would have been obvious to one of ordinary skill in the art at the

time of invention to add or make use of digital signatures in sending authenticated digital content request messages by the user devices of the combined invention of De Jong et al. and Barrus et al. because unique identifiers such as the MAC address of a user device requesting digital content can be used to generate a "digital signature" to be packaged as a token along with the message as taught by Barrus et al. (US 2003/0204721 A1, Pg 3, Par 0029). As such the method further comprising an act of authenticating at least one of the one or more digital signatures would have been inherent for combining the use of digital signatures for authentication. The suggestion/motivation for combining would have been to provide another layer of security for secured transaction by authenticating the creator of the signature (the digital content requestor in this case) which is well known in the art of digital security. Therefore, it would have been obvious to combine the use of digital signatures for authentication in the combined inventions of de Jong et al. and Barrus et al.

Regarding claim 3, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 1, further comprising an act of receiving a message from a sending computer system [de Jong et al. teach user devices sending authenticated digital content request message with one or more security tokens to Content Repository via a Portal (US 2004/0054628 A1, Fig 8)], the message including an encrypted portion and one or more security tokens [Barrus et al. teach encrypting the message with a security token (US 2003/0204721 A1, Pg 1, Par 0010).].

Regarding claim 5, the use of binary security tokens in the method as recited in claim 1 are inherent when using Web Services Security as taught by the combined inventions of de Jong et al. and Barrus et al. [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 6, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 1, wherein the identified corresponding value type is a custom value type created by the sending computer system or the receiving computer system, and that the receiving and sending computer system can access [The Synchronizer manages token pool information which is information about tokens being created, accessed, and used in the system by the receiving and sending entities of digital content requests (US 2004/0054628 A1, Pg 9, Par 0133)].

Regarding claim 7, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 1, further comprising an act of updating one or more properties of the stored security token that is accessible by the receiving computer system with one or more of the identification information and the custom property [The Synchronizer manages token pool information which is information about tokens being created, accessed, and used in the system by the receiving and sending entities of digital content requests (US 2004/0054628 A1, Pg 9, Par 0133).].

Regarding claim 8, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 7, further comprising an act of creating a security key when

updating the one or more properties of the stored security token [A token chain key is created when a new token chain is being generated because of updated token properties/specifications/parameters. A token pool key is also created when new tokens or token chains or token pools are generated. (US 2004/0054628 A1, Pg 10, Par 0140) (US 2004/0054628 A1, Fig 20)].

Regarding claim 9, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 1, wherein the identified at least one security token is serialized in the received message based on a private key that is shared between the sending and receiving computer system [Token chain keys are shared between sending and receiving entities of authenticated digital content requests. (US 2004/0054628 A1, Pg 11, Par 0152)].

Regarding claim 10, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 9, wherein the private key is accessed from a key provider that both the sending and the receiving computer systems can access [The Synchronizer is the key provider and synchronization of token pool information that can be accessed by sending and receiving authenticated digital content request entities through internal requests for synchronization (US 2004/0054628 A1, Pg 18, Par 0213)].

Regarding claim 11, the method as recited in claim 1, wherein the one or more security tokens are found in a security header portion of the message are inherent when using

Web Services Security communications protocol as taught by the combined inventions of de Jong et al. and Barrus et al. [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 12, the method as recited in claim 11, wherein, prior to receiving the message, the at least one identified token is serialized into the security header portion of the message by transforming the at least one identified security token into base 64 encoded data is inherent because this type of encoding is built into the Web Services Security communications protocol and such communications protocol is taught by the combined inventions of de Jong et al. and Barrus et al. [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 13, the method as recited in claim 12, wherein deserializing comprises an act of converting data from the identified at least one token from base 64 encoding to a byte array is inherent because this type of decoding is built into the Web Services Security communications protocol and such communications protocol is taught by the combined inventions of de Jong et al. and Barrus et al. [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 14, this claim is rejected using the same references and rationale of claims 1, 11, and 12.

Regarding claim 17, de Jong et al. teach a computerized network environment including

two or more computer systems sending messages through a network communication protocol, a method of sending secure messages using custom security tokens, the method comprising: an act of a sending computer system generating one or more security tokens using one or more corresponding value types, each token including token data that includes one or more of a custom property, a signature, and an encryption level [(US 2004/0054628 A1, Pg 7, Par 0111-0112), (US 2004/0054628 A1, Pg 7, Par 0137), Data regarding encryption level is inherent in a system implementing an encryption/decryption process. A cryptogram may authenticate the protected digital content or a reference to the protected digital content (which by definition is a type of signature).]; an act of encrypting a portion of a message using at least one of the one or more generated security tokens; an act of inserting the at least one generated security token in an outbound token collection [Security tokens are organized into chains and or pools. (US 2004/0054628 A1, Pg 7, Par 0140)], wherein the act of inserting the at least one generated security token in an outbound token collection further comprises:

an act of identifying a markup language representation of the at least one generated security token [Token Chain ID, offset, token type indicator, (Pg 10, Par 0137) – the act of identifying is inherent.], and an act of placing the markup language representation of the at least one generated security token in the outbound token collection [(US 2004/0054628 A1, Pg 7, starting Par 0140) Such representation is inherent in the token pool information.]; and an act of converting the token data for the outbound token collection using a private key that is accessible by the sending computer system and a receiving computer system [(US 2004/0054628 A1, Pg 7,

starting Par 0140) Such a private key is the token pool key, or the token chain key depending on which perspective.]. de Jong et al does not teach the act of encrypting a portion of a message using at least one of the one or more generated security tokens. Barrus et al. teaches the act of encrypting a portion of a message using at least one of the one or more generated security tokens [Pg 1, Par 0010].

It would have been obvious to one of ordinary skill in the art at the time of invention to add another layer of security in the method of sending authenticated digital content request of de Jong et al. by using additional security tokens to encrypt digital content request messages as taught by Barrus et al. because authenticated digital content request has information that include token pool information used for validation [US 2004/0054628 A1, Pg 6, Par 0101] that can be encrypted using additional security tokens to enable a more secure transaction between requesting user media devices and content providers. The suggestion/motivation for combining would have been to prevent an entity other than the intended recipient from accessing the message [US 2003/0204721 A1] thereby protecting the user's interest since an authenticated digital content request has information about the user's token pool. De Jong et al. and Barrus et al. are analogous art because they are both in the same field of endeavor involving messaging using security tokens. Therefore, it would have been obvious to combine the inventions of De Jong et al. and Barrus et al.

Regarding claim 18, the use of digital signatures for authentication is well known in the art of digital security. It would have been obvious to one of ordinary skill in the art at the

time of invention to add or make use of digital signatures in sending authenticated digital content request messages by the user devices of the combined invention of De Jong et al. and Barrus et al. because unique identifiers such as the MAC address of a user device requesting digital content can be used to generate a "digital signature" to be packaged as a token along with the message as taught by Barrus et al. (US 2003/0204721 A1, Pg 3, Par 0029). As such the method further comprising an act of authenticating the one or more digital signatures prior to decrypting the encrypted portion of the message would have been inherent for combining the use of digital signatures for authentication. The suggestion/motivation for combining would have been to provide another layer of security for secured transaction by authenticating the creator of the signature (the digital content requestor in this case) which is well known in the art of digital security. Therefore, it would have been obvious to combine the use of digital signatures for authentication in the combined inventions of de Jong et al. and Barrus et al.

Regarding claim 19, the combined inventions of de Jong et al. and Barrus et al. teach The method as recited in claim 17, further comprising an act of including private key information in the message, such that the receiving computer system can access the key from a key provider based on the key information [The Synchronizer is the key provider and synchronization of token pool information and keys that can be accessed by sending and receiving authenticated digital content request entities through internal requests for synchronization (US 2004/0054628 A1, Pg 18, Par 0213)].

Regarding claim 20, the method as recited in claim 17, wherein the act of converting the token data comprises serializing the token data into base 64 encoding is inherent because this type of encoding is built into the Web Services Security communications protocol and such communications protocol is taught by the combined inventions of de Jong et al. and Barrus et al. [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 21, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 17, wherein the at least one generated security token is a custom security token created using a custom value type, and wherein the custom value type is accessible by both the sending and receiving computer systems [The Synchronizer manages token pool information which is information about tokens being created, accessed, and used in the system by the receiving and sending entities of digital content requests (US 2004/0054628 A1, Pg 9, Par 0133)].

Regarding claim 22, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 17, further comprising an act of creating a signature or encryption function based on the included one or more of a custom property, a signature, and an encryption level in the created binary token [US 2004/0054628 A1, Fig 19].

Regarding claims 23 and 24, the combined inventions of de Jong et al. and Barrus et al.

teach the method as recited in claim 17, further comprising an act of including a program language value corresponding with each token that is included in the outbound token collection and wherein the program language value is a Common Language Runtime value [(US 2004/0054628 A1, Pg 8, starting Par 0118) du Jong et al. teach "servlet"(s) that can handle the common language infrastructure.].

Regarding claim 26, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 17, further comprising an act of assigning the markup language representation of the at least one generated security token a global unique identifier [A global unique identifier is interpreted as a type of identifier known across all platforms or throughout entire network system. Since tokens are implemented using URLs, many or all can qualify as a global unique identifier.]

Regarding claim 27, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 26, wherein the outbound token collection is a hash table that is keyed by the global unique identifier of the at least one generated security token [(US 2004/0054628 A1, Pg 10, Par 0140-141) Since the cryptographic process includes a hashing function, the resulting encryption process can be interpreted as a hashing table since tokens taught by de Jong et al. is also organized in a data structure ie. pools and chains. Many identifiers used by de Jong et al. qualify as the global unique identifier such as the Seed or the last token identifier (since the last token identifier in

one embodiment is used to generate the token chain).].

Regarding claim 28, the combined inventions of de Jong et al. and Barrus et al. teach the method as recited in claim 27, wherein the global unique identifier is inserted into a signature or encryption portion of the message.

Claim 29 and 33 is rejected using references and rationale of claims 17, 19, 23, and 24.

Regarding claim 32, the method as recited in claim 14, wherein deserializing comprises an act of converting data from the identified at least one token from base 64 encoding to a byte array is inherent because this type of decoding is built into the Web Services Security communications protocol and such communications protocol is taught by the combined inventions of de Jong et al. and Barrus et al. [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Jeriko P. San Juan whose telephone number is 571-272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/

Martin Jeriko San Juan

Examiner. Art Unit 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100